

DETAILED ACTION

1. Claims 1-15 are pending.
2. Preliminary Amendment filed 06/15/2005 has been received and considered.

Claim Objections

3. Claim 1 is objected to because of the following informalities: claim 1 line 10 states "encrypted images" however only a single "encrypted image" is disclosed in the claim. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
6. Regarding claim 15, the word "preferably" renders the claim indefinite because it is unclear whether the limitation

Art Unit: 2137

following the word is part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1, 5, 7 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tehranchi (US 7242772) in view of Fan et al. (US 5541993) and further in view of Imai (US 5512977).

As per claims 1 and 7, Tehranchi teaches a method and device for synchronizing a first key set in an encryption device and a second key set in a decryption device, the method comprising the steps of: the encryption device producing an encrypted image (see column 7 lines 22-32 and lines 40-51) and an associated key identification using a key of the first key set (see column 8 lines 7-41 and column 9 lines 15-23 where the synchronization information shown in FIG. 3 has the key identification, the frame number, and the associated key of the

Art Unit: 2137

set of keys), the encryption device transmitting the encrypted image and its associated key identification to a display device (see column 7 lines 53-64), the decryption device detecting the key identification (see column 9 lines 42-51), the decryption device decrypting the encrypted image using a key of the second key set corresponding with the detected key identification, and the decryption device displaying the decrypted image (see column 8 line 53 through column 9 line 4 where the destination site with the projector is the "decryption device").

Tehranchi fails to disclose the display device displaying the encrypted image and its associated key identification.

However, Fan et al. teaches displaying and encrypted image (see column 3 lines 25-27) and Imai teaches displaying a key identification associated with specific data (see column 4 lines 48-59).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to display the encrypted images and their associated key identification of the Tehranchi system.

Motivation to do so would have been to verify that the image was properly encrypted (see Fan et al. column 8 line 56 through column 9 line 14) and to allow the correct key identification to be chosen (see Imai column 4 lines 48-59).

As per claims 5 and 11, the modified Tehranchi, Fan et al. and Imai system discloses the key identification is part of the encrypted image (see Tehranchi column 9 lines 39-65 where the frame number or frame component ID, which is part of each encrypted frame, is used to find the correct key).

9. Claims 2, 3, 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Tehranchi, Fan et al. and Imai system as applied to claims 1 and 7 above, and further in view of Price, III (US 6851049).

As per claims 2, 3, 8, and 9, the modified Tehranchi, Fan et al. and Imai system fails to disclose the key identification is a code derived from the key that is a hash value.

However, Price, III teaches taking a hash value of a key for the key identification (see column 4 lines 42-54).

At the time of the invention it would have been obvious to a person of ordinary skill in the art for the key identification (i.e. the frame number) of the modified Tehranchi, Fan et al. and Imai system to be formed by applying a hash function to the key.

Motivation to do so would have been to have a key identification that is of uniform length and statistically unique (see Price, III column 4 lines 50-54).

Art Unit: 2137

10. Claims 4 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Tehranchi, Fan et al., Imai, and Price, III system as applied to claims 3 and 9 above, and further in view of Barrett et al. (US 5185797).

As per claims 4 and 10, the modified Tehranchi, Fan et al., Imai and Price, III system discloses using a key identifier that is a hash value of the key to synchronize an encryption system (see specifically Tehranchi and Prince, II as applied above), but fails to explicitly disclose the decryption device detecting the hash value and storing it as a detected hash value, the decryption device calculating the hash values of the second key set and comparing each calculated hash value with the detected hash value until a match is found.

However, Barrett et al. teaches a key synchronization system that compares a received key ID against all stored values associated with its key set (see column 9 lines 39-56 where the received key, i.e. the key ID field 100, must be stored in order to do any type of comparison).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to search all of the key Ids of the modified Tehranchi, Fan et al., Imai and Price, III system.

Motivation to do so would have been to determine if the device is capable of decrypting the received information (see Barrett et al. column 9 lines 39-56).

11. Claims 6, 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Tehranchi, Fan et al. and Imai system as applied to claims 1 and 7 above, and further in view of Jones (US 20020101988).

As per claims 6 and 12, the modified Tehranchi, Fan et al. and Imai system fails to disclose the key identification is displayed on the display device as a bar code and/or a time multiplexed code.

However, Jones teaches displaying information related to encryption/decryption on a display device as a bar code (see paragraphs [0033] and [0036]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to display the key identification of the modified Tehranchi, Fan et al. and Imai system as a bar code.

Motivation to do so would have been to allow for a machine (i.e. bar code reader) to easily read the value (see Jones paragraph [0036]).

As per claim 13, the modified Tehranchi, Fan et al. and Imai system discloses a device comprising means for detecting an

Art Unit: 2137

encrypted image and a key identification, key selection means for selecting a key on the basis of the sensed key identification, decryption means for decrypting a sensed encrypted image using the selected key, and display means for displaying a decrypted image (see Tehranchi column 7 lines 53-64; column 8 line 53 through column 9 line 4; and column 9 lines 42-51), but fails to disclose the specific sensing means.

However, Jones teaches means for sensing an encrypted image and additional information (see paragraphs [0005], [0033] and [0036]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the means of Jones to sense the encrypted image and its associated key identification of the modified Tehranchi, Fan et al. and Imai system.

Motivation to do so would have been to only allow users with the specific means to render the encrypted images viewable (see Jones paragraph [0005]).

12. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Tehranchi, Fan et al., Imai and Jones system as applied to claim 13 above, and further in view of Miguel et al. (US 5593349).

As per claims 14 and 15, the modified Tehranchi, Fan et al., Imai and Jones system discloses the use of a barcode reader as part of the sensor means (see Jones paragraph [0036], but fails to disclose the sensor means are constituted by photo diodes and are part of an LED circuit.

However, Miguel et al. teaches the use of photo diodes and an LED circuit as part of a barcode reader (see column 10 lines 41-64).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include photo diodes and an LED circuit as part of the sensor means of the modified Tehranchi, Fan et al., Imai and Jones system.

Motivation, as recognized by one of ordinary skill in the art, to do so would have been that this is a common and well-known method of detecting barcodes.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Schrijen et al. teaches a method of key synchronization for encrypted images; Matsumoto et al. teaches the use of a hash on an encryption key to determine a key ID; Gilbert et al. teaches checking key IDs

until a match is found; and Walsh et al. teaches another convention barcode reader.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/539,359
Art Unit: 2137

Page 11

/Michael Pyzocha/
Examiner, Art Unit 2137